

MAIL STOP PATENT APPLICATION

Attorney Docket No. 25880

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Yuuki MIYAZAKI

Serial No. NOT YET ASSIGNED

Filed: December 15, 2003

For: **LICENSE MANAGEMENT METHOD AND LICENSE MANAGEMENT SYSTEM**

REQUEST FOR PRIORITY UNDER 35 U.S.C. §119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In the matter of the above-captioned application, notice is hereby given that the Applicant claims as priority date December 25, 2002, the filing date of the corresponding application filed in JAPAN, bearing Application Number P2002-374970.

A Certified Copy of the corresponding application is submitted herewith.

Respectfully submitted,
NATH & ASSOCIATES PLLC

Date: December 15, 2003

By: 

Gary M. Nath
Reg. No. 26,965
Marvin C. Berkowitz
Reg. No. 47,421
Customer No. 20529

NATH & ASSOCIATES PLLC
6TH Floor
1030 15th Street, N.W.
Washington, D.C. 20005
(202)-775-8383
GMN/MCB/dd (Priority)

JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: December 25, 2002

Application Number: P2002-374970

[ST.10/C]: [JP2002-374970]

Applicant(s): VICTOR COMPANY OF JAPAN, LIMITED

October 17, 2003

Commissioner,

Japan Patent Office Yasuo IMAI

Number of Certificate: 2003-3085807

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年12月25日
Date of Application:

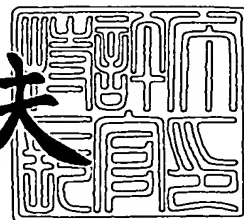
出願番号 特願2002-374970
Application Number:
[ST. 10/C]: [JP2002-374970]

出願人 日本ビクター株式会社
Applicant(s):

2003年10月17日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3085807

【書類名】 特許願

【整理番号】 414001185

【提出日】 平成14年12月25日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 17/60

【発明の名称】 ライセンス管理方法、およびライセンス管理システム

【請求項の数】 6

【発明者】

【住所又は居所】 神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地 日本ビクター株式会社内

【氏名】 宮崎 優樹

【特許出願人】

【識別番号】 000004329

【氏名又は名称】 日本ビクター株式会社

【代理人】

【識別番号】 100083806

【弁理士】

【氏名又は名称】 三好 秀和

【電話番号】 03-3504-3075

【選任した代理人】

【識別番号】 100068342

【弁理士】

【氏名又は名称】 三好 保男

【選任した代理人】

【識別番号】 100101247

【弁理士】

【氏名又は名称】 高橋 俊一

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9802012

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ライセンス管理方法、およびライセンス管理システム

【特許請求の範囲】

【請求項 1】 ソフトウェア製品を識別する識別コードを発行する製品管理サーバと、前記識別コードとユーザ端末を識別する端末コードとを含むライセンス情報を記録するデータベースを備え、前記ユーザ端末から送信される情報と前記ライセンス情報とを照合する認証サーバと、認証の基準となるデジタル署名を作成するルートサーバとから構成されるライセンス管理システムにおいて、ユーザ端末にインストールされるソフトウェアのライセンス管理を公開鍵暗号方式の秘密鍵と公開鍵とを用いて行うライセンス管理方法であって、

前記製品管理サーバにおいて、前記製品管理サーバの秘密鍵を用いて、前記識別コードから前記ソフトウェア製品に付される第 1 のデジタル署名を作成する第 1 のデジタル署名作成工程と、

前記ルートサーバにおいて、前記製品管理サーバから前記製品管理サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記製品管理サーバの公開鍵から第 2 のデジタル署名を作成する第 2 のデジタル署名作成工程と、

前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵から第 3 のデジタル署名を作成する第 3 のデジタル署名作成工程と、

前記認証サーバにおいて、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第 2 のデジタル署名の正否を判定し、判定結果に基づいて前記製品管理サーバの公開鍵を取得する第 1 の判定工程と、

前記認証サーバにおいて、前記ユーザ端末から第 1 のデジタル署名と前記端末コードとを受信すると、前記製品管理サーバの公開鍵を用いて前記第 1 のデジタル署名の正否を判定し、判定結果に基づいて前記識別コードを取得する第 2 の判定工程と、

前記認証サーバにおいて、前記識別コードと前記端末コードとを前記データベースに記録されているライセンス情報と照合し、所定の条件に該当する場合は、当該識別コードと当該端末コードとを前記データベースに記録する記録工程と、

前記認証サーバにおいて、前記認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードとから第 4 のデジタル署名を作成する第 4 のデジタル署名作成工程と、

前記ユーザ端末において、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第 3 のデジタル署名の正否を判定し、判定結果に基づいて前記認証サーバの公開鍵を取得する第 3 の判定工程と、

前記ユーザ端末において、前記第 3 の判定工程において取得された前記認証サーバの公開鍵を用いて前記第 4 のデジタル署名の正否を判定し、判定結果に基づいて前記製品識別コードと前記端末コードを取得する第 4 の判定工程と、

前記ユーザ端末において、前記第 4 の判定工程の判定結果に基づいて、前記ソフトウェアの機能制限を解除する制限解除工程と、

を有することを特徴とするライセンス管理方法。

【請求項 2】 前記認証サーバは、前記第 3 のデジタル署名の有効期限を示すサーバ有効期限を有し、

前記第 3 のデジタル署名作成工程では、前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵と前記サーバ有効期限とを取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵と前記サーバ有効期限とから認証サーバのデジタル署名を作成し、

前記第 3 の判定工程では、前記ユーザ端末において、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記認証サーバのデジタル署名の正否を判定し、前記サーバ有効期限と前記認証サーバの公開鍵とを取得し、

前記第 3 の判定工程で正当と判定された前記サーバ有効期限と現在の日付とを照合する照合工程を有することを特徴とする請求項 1 に記載のライセンス管理方法。

【請求項 3】 前記認証サーバは、ソフトウェアの使用期限を示すソフト有効期限を有し、

前記第 4 のデジタル署名作成工程では、認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードと前記ソフト有効期限とから端末のデジタル署名を作成し、

前記第4の判定工程では、前記ユーザ端末において、前記認証サーバから取得する前記認証サーバの公開鍵を用いて前記第4のデジタル署名の正否を判定し、前記製品コードと前記端末コードと前記ソフト有効期限とを取得し、

前記制限解除工程では、前記第4の判定工程で正当と判定された前記ソフト有効期限に基づいて、インストールされた前記ソフトウェアの機能制限を解除することを特徴とする請求項1または請求項2に記載のライセンス管理方法。

【請求項4】 ソフトウェア製品がインストールされるユーザ端末と、前記ソフトウェア製品を識別する識別コードを発行する製品管理サーバと、前記識別コードと前記ユーザ端末を識別する端末コードとを含むライセンス情報を記録するデータベースを備え、前記ユーザ端末から送信される情報と前記ライセンス情報とを照合する認証サーバと、認証の基準となるデジタル署名を作成するルートサーバとから構成されるライセンス管理システムであって、

前記製品管理サーバは、

前記製品管理サーバの秘密鍵を用いて、前記識別コードから前記ソフトウェア製品に付される第1のデジタル署名を作成する第1のデジタル署名作成手段、
を備え、

前記ルートサーバは、

前記製品管理サーバから前記製品管理サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記製品管理サーバの公開鍵から第2のデジタル署名を作成する第2のデジタル署名作成手段と、

前記認証サーバから前記認証サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵から第3のデジタル署名を作成する第3のデジタル署名作成手段と、

を備え、

前記認証サーバは、

前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第2のデジタル署名の正否を判定し、判定結果に基づいて前記製品管理サーバの公開鍵を取得する第1の判定手段と、

前記ユーザ端末から第1のデジタル署名と前記端末コードとを受信すると、前

記製品管理サーバの公開鍵を用いて前記第 1 のデジタル署名の正否を判定し、判定結果に基づいて前記識別コードを取得する第 2 の判定手段と、

前記識別コードと前記端末コードとを前記データベースに記録されているライセンス情報と照合し、所定の条件に該当する場合は、当該識別コードと当該端末コードとを前記データベースに記録する記録手段と、

前記認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードとから第 4 のデジタル署名を作成する第 4 のデジタル署名作成手段と、

を備え、

前記ユーザ端末は、

前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第 3 のデジタル署名の正否を判定し、判定結果に基づいて前記認証サーバの公開鍵を取得する第 3 の判定手段と、

前記第 3 の判定手段によって取得された前記認証サーバの公開鍵を用いて前記第 4 のデジタル署名の正否を判定し、判定結果に基づいて前記製品識別コードと前記端末コードを取得する第 4 の判定手段と、

前記第 4 の判定手段の判定結果に基づいて、前記ソフトウェアの機能制限を解除する制限解除手段と、

を備えることを特徴とするライセンス管理システム。

【請求項 5】 前記認証サーバは、前記第 3 のデジタル署名の有効期限を示すサーバ有効期限を有し、

前記第 3 のデジタル署名作成手段は、前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵と前記サーバ有効期限とを取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵と前記サーバ有効期限とから認証サーバのデジタル署名を作成し、

前記ユーザ端末において、前記第 3 の判定手段は、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記認証サーバのデジタル署名の正否を判定し、前記サーバ有効期限と前記認証サーバの公開鍵とを取得し、

前記第 3 の判定手段で正当と判定された前記サーバ有効期限と現在の日付とを照合する照合手段を有することを特徴とする請求項 4 に記載のライセンス管理シ

ステム。

【請求項 6】 前記認証サーバは、ソフトウェアの使用期限を示すソフト有効期限を有し、

前記第 4 のデジタル署名作成手段は、認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードと前記ソフト有効期限とから端末のデジタル署名を作成し、

前記ユーザ端末において、前記第 4 の判定手段は、前記認証サーバから取得する前記認証サーバの公開鍵を用いて前記第 4 のデジタル署名の正否を判定し、前記製品コードと前記端末コードと前記ソフト有効期限とを取得し、

前記制限解除手段は、前記第 4 の判定手段で正当と判定された前記ソフト有効期限に基づいて、インストールされた前記ソフトウェアの機能制限を解除することを特徴とする請求項 4 または請求項 5 に記載のライセンス管理システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ソフトウェアのライセンス管理を公開鍵暗号方式の秘密鍵と公開鍵とを用いて行うライセンス管理方法およびライセンス管理システムに関する。

【0002】

【従来の技術】

一般的に、ソフトウェアは、CD-ROM等の記憶媒体に記憶させた形で提供されたり、インターネットを通じてダウンロードする形でユーザに提供されたりする。このようなソフトウェアは容易に複製が可能であり、そのため実際には1本のソフトウェアがコピーされて、複数のコンピュータで不正に使用されることがある。

【0003】

このような不正使用を防止するため、従来、ライセンスコードを用いる方法がある。この方法では、ライセンスコードをソフトウェアの販売時に添付したり、入金された時にユーザに伝えたりしてユーザに渡し、ユーザはソフトウェアをインストールする際にライセンスコードを入力する。このライセンスコードをソフ

トウェアで認証することによって正規ユーザであるかどうかを確認することができる。

【0004】

しかし、この方法では、ライセンスコードを知りさえすれば、不正にコピーしたソフトウェアを使用することが可能である。またライセンスコードの生成パターンが流出すると、新たなライセンスコードが不正に生成され、正規のライセンスコードを知らなくてもソフトウェアを不正に使用することが可能となってしまう。逆に、ライセンスコードを高度に複雑化すれば、ユーザの操作が煩雑となる。従って、この方法では、不正使用に対して十分な効果が発揮できなかった。

【0005】

これに対し、販売管理サーバとライセンス管理サーバを用いて認証をソフトウェアの管理を行う方法も提案されている（例えば、特許文献1）。この方法では、販売管理サーバがユーザに対してライセンスコードを発行すると共に、ライセンス管理サーバに対して発行履歴をライセンス管理サーバに通知する。ユーザはライセンスコードとマシン識別コードをライセンス管理サーバに通知すると、ライセンスコードを発行履歴と照合して、問題がなければソフトウェア使用キーを発行する。従って、ライセンスコードの発行履歴を確認でき、またマシン識別コードによってユーザを識別できるので、不正なコピーを防止できる。

【0006】

【特許文献1】

特開2000-207199号公報

【0007】

【発明が解決しようとする課題】

しかしながら、この方法では、販売管理サーバやライセンス管理サーバに対する認証を行っていないため、不正なユーザに対しては有効であるが、販売管理サーバやライセンス管理サーバが不正な場合には、不正を防止することができなかった。

【0008】

例えば、販売管理サーバを不正に設け、ライセンスコードを発行して販売管理

サーバに通知した場合、これを発見することができない。またライセンス管理サーバのソフトウェア使用キーの生成方法が流出し、ライセンス管理サーバを不正に設けられた場合、これを発見することはできない。このように、販売管理サーバやライセンス管理サーバに不正があった場合、これを防止することができないという問題があった。

【0009】

本発明は上記事情に鑑み、ユーザ端末にインストールされるソフトウェアのライセンス管理を公開鍵暗号方式の秘密鍵と公開鍵とを用いて行うライセンス管理方法、およびライセンス管理システムを提供することを目的とする。

【0010】

【課題を解決するための手段】

上記目的を達成するために、請求項1に記載の発明であるライセンス管理方法は、ソフトウェア製品を識別する識別コードを発行する製品管理サーバと、前記識別コードとユーザ端末を識別する端末コードとを含むライセンス情報を記録するデータベースを備え、前記ユーザ端末から送信される情報と前記ライセンス情報とを照合する認証サーバと、認証の基準となるデジタル署名を作成するルートサーバとから構成されるライセンス管理システムにおいて、ユーザ端末にインストールされるソフトウェアのライセンス管理を公開鍵暗号方式の秘密鍵と公開鍵とを用いて行うライセンス管理方法であって、前記製品管理サーバにおいて、前記製品管理サーバの秘密鍵を用いて、前記識別コードから前記ソフトウェア製品に付される第1のデジタル署名を作成する第1のデジタル署名作成工程と、前記ルートサーバにおいて、前記製品管理サーバから前記製品管理サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記製品管理サーバの公開鍵から第2のデジタル署名を作成する第2のデジタル署名作成工程と、前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵から第3のデジタル署名を作成する第3のデジタル署名作成工程と、前記認証サーバにおいて、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第2のデジタル署名の正否を判定し、判定結果に基づいて前記製品管理サーバの公開鍵を取得する第1

の判定工程と、前記認証サーバにおいて、前記ユーザ端末から第1のデジタル署名と前記端末コードとを受信すると、前記製品管理サーバの公開鍵を用いて前記第1のデジタル署名の正否を判定し、判定結果に基づいて前記識別コードを取得する第2の判定工程と、前記認証サーバにおいて、前記識別コードと前記端末コードとを前記データベースに記録されているライセンス情報と照合し、所定の条件に該当する場合は、当該識別コードと当該端末コードとを前記データベースに記録する記録工程と、前記認証サーバにおいて、前記認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードとから第4のデジタル署名を作成する第4のデジタル署名作成工程と、前記ユーザ端末において、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第3のデジタル署名の正否を判定し、判定結果に基づいて前記認証サーバの公開鍵を取得する第3の判定工程と、前記ユーザ端末において、前記第3の判定工程において取得された前記認証サーバの公開鍵を用いて前記第4のデジタル署名の正否を判定し、判定結果に基づいて前記製品識別コードと前記端末コードとを取得する第4の判定工程と、前記ユーザ端末において、前記第4の判定工程の判定結果に基づいて、前記ソフトウェアの機能制限を解除する制限解除工程とを有することを特徴とする。

【0011】

請求項1の発明によれば、ソフトウェア固有の識別コードやユーザ端末固有の端末コードを用いて、製品管理サーバの暗号鍵と認証サーバの暗号鍵をルートサーバで認証してから使用するので、ソフトウェアの偽造、改ざんだけでなく、暗号鍵の偽造、改ざん、偽の製品管理サーバ、偽の認証サーバなどに対しても対抗できる、不正行為を防止するソフトウェアのライセンス管理が可能となる。

【0012】

また、請求項2に記載の発明であるライセンス管理方法は、請求項1に記載のライセンス管理方法であって、前記認証サーバは、前記第3のデジタル署名の有効期限を示すサーバ有効期限を有し、前記第3のデジタル署名作成工程では、前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵と前記サーバ有効期限とを取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵と前記サーバ有効期限とから認証サーバのデジタル署名を作成し、前記

第3の判定工程では、前記ユーザ端末において、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記認証サーバのデジタル署名の正否を判定し、前記サーバ有効期限と前記認証サーバの公開鍵とを取得し、前記第3の判定工程で正当と判定された前記サーバ有効期限と現在の日付とを照合する照合工程を有することを特徴とする。

【0013】

請求項2の発明によれば、第3のデジタル署名の有効期限を示すサーバ有効期限を設定しているので、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたサーバ有効期限で無効となるので、不正使用を一時的なものにすることができる。

【0014】

また、請求項3に記載の発明であるライセンス管理方法は、請求項1または請求項2に記載のライセンス管理方法であって、前記認証サーバは、ソフトウェアの使用期限を示すソフト有効期限を有し、前記第4のデジタル署名作成工程では、認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードと前記ソフト有効期限とから端末のデジタル署名を作成し、前記第4の判定工程では、前記ユーザ端末において、前記認証サーバから取得する前記認証サーバの公開鍵を用いて前記第4のデジタル署名の正否を判定し、前記製品コードと前記端末コードと前記ソフト有効期限とを取得し、前記制限解除工程では、前記第4の判定工程で正当と判定された前記ソフト有効期限に基づいて、インストールされた前記ソフトウェアの機能制限を解除することを特徴とする。

【0015】

請求項3の発明によれば、ソフトウェアの使用期限を示すソフト有効期限が切れると再びアクティベーションを促すようにしておけば、ユーザは再びアクティベーションを行うこととなり、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたソフト有効期限で機能が停止するので、不正使用を一時的なものにすることができる。

【0016】

また、請求項4に記載の発明であるライセンス管理システムは、ソフトウェア

製品がインストールされるユーザ端末と、前記ソフトウェア製品を識別する識別コードを発行する製品管理サーバと、前記識別コードと前記ユーザ端末を識別する端末コードとを含むライセンス情報を記録するデータベースを備え、前記ユーザ端末から送信される情報と前記ライセンス情報とを照合する認証サーバと、認証の基準となるデジタル署名を作成するルートサーバとから構成されるライセンス管理システムであって、前記製品管理サーバは、前記製品管理サーバの秘密鍵を用いて、前記識別コードから前記ソフトウェア製品に付される第1のデジタル署名を作成する第1のデジタル署名作成手段を備え、前記ルートサーバは、前記製品管理サーバから前記製品管理サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記製品管理サーバの公開鍵から第2のデジタル署名を作成する第2のデジタル署名作成手段と、前記認証サーバから前記認証サーバの公開鍵を取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵から第3のデジタル署名を作成する第3のデジタル署名作成手段とを備え、前記認証サーバは、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第2のデジタル署名の正否を判定し、判定結果に基づいて前記製品管理サーバの公開鍵を取得する第1の判定手段と、前記ユーザ端末から第1のデジタル署名と前記端末コードとを受信すると、前記製品管理サーバの公開鍵を用いて前記第1のデジタル署名の正否を判定し、判定結果に基づいて前記識別コードを取得する第2の判定手段と、前記識別コードと前記端末コードとを前記データベースに記録されているライセンス情報と照合し、所定の条件に該当する場合は、当該識別コードと当該端末コードとを前記データベースに記録する記録手段と、前記認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードとから第4のデジタル署名を作成する第4のデジタル署名作成手段とを備え、前記ユーザ端末は、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記第3のデジタル署名の正否を判定し、判定結果に基づいて前記認証サーバの公開鍵を取得する第3の判定手段と、前記第3の判定手段によって取得された前記認証サーバの公開鍵を用いて前記第4のデジタル署名の正否を判定し、判定結果に基づいて前記製品識別コードと前記端末コードとを取得する第4の判定手段と、前記第4の判定手段の判定結果に基づいて、前記ソフトウェアの機能制限を解除する制限解除

手段とを備えることを特徴とする。

【0017】

請求項4の発明によれば、ソフトウェア固有の識別コードやユーザ端末固有の端末コードを用いて、製品管理サーバの暗号鍵と認証サーバの暗号鍵をルートサーバで認証してから使用するので、ソフトウェアの偽造、改ざんだけでなく、暗号鍵の偽造、改ざん、偽の製品管理サーバ、偽の認証サーバなどに対しても対抗できる、不正行為を防止するソフトウェアのライセンス管理が可能となる。

【0018】

また、請求項5に記載の発明であるライセンス管理システムは、請求項4に記載のライセンス管理システムであって、前記認証サーバは、前記第3のデジタル署名の有効期限を示すサーバ有効期限を有し、前記第3のデジタル署名作成手段は、前記ルートサーバにおいて、前記認証サーバから前記認証サーバの公開鍵と前記サーバ有効期限とを取得し、前記ルートサーバの秘密鍵を用いて、前記認証サーバの公開鍵と前記サーバ有効期限とから認証サーバのデジタル署名を作成し、前記ユーザ端末において、前記第3の判定手段は、前記ルートサーバから取得する前記ルートサーバの公開鍵を用いて前記認証サーバのデジタル署名の正否を判定し、前記サーバ有効期限と前記認証サーバの公開鍵とを取得し、前記第3の判定手段で正当と判定された前記サーバ有効期限と現在の日付とを照合する照合手段を有することを特徴とする。

【0019】

請求項5の発明によれば、第3のデジタル署名の有効期限を示すサーバ有効期限を設定しているので、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたサーバ有効期限で無効となるので、不正使用を一時的なものにすることができる。

【0020】

また、請求項6に記載の発明であるライセンス管理システムは、請求項4または請求項5に記載のライセンス管理システムであって、前記認証サーバは、ソフトウェアの使用期限を示すソフト有効期限を有し、前記第4のデジタル署名作成手段は、認証サーバの秘密鍵を用いて、前記製品コードと前記端末コードと前記

ソフト有効期限とから端末のデジタル署名を作成し、前記ユーザ端末において、前記第4の判定手段は、前記認証サーバから取得する前記認証サーバの公開鍵を用いて前記第4のデジタル署名の正否を判定し、前記製品コードと前記端末コードと前記ソフト有効期限とを取得し、前記制限解除手段は、前記第4の判定手段で正当と判定された前記ソフト有効期限に基づいて、インストールされた前記ソフトウェアの機能制限を解除することを特徴とする。

【0021】

請求項6の発明によれば、ソフトウェアの使用期限を示すソフト有効期限が切れると再びアクティベーションを促すようにしておけば、ユーザは再びアクティベーションを行うこととなり、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたソフト有効期限で機能が停止するので、不正使用を一時的なものにすることができる。

【0022】

【発明の実施の形態】

本発明の実施の形態を説明するにあたって、まず、図9を用いて、公開鍵暗号方式の認証の原理を説明する。

【0023】

ソフトウェア作成者の手元には、秘密鍵D61と公開鍵E62との一組の鍵があり、秘密鍵D61と復号化アルゴリズムAとを利用して、メッセージ（ソフトウェア）M63からデジタル署名S64（ $S = A(D, M)$ ）が作成され（ステップS71）、メッセージM63とデジタル署名S64をまとめた証明書データL65（ $L = (M, S)$ ）が作成される（ステップS72）。作成された証明書データL65はソフトウェア利用者側に送信される（ステップS73）。また、公開鍵E62は、不特定多数に公開されるものとする。

【0024】

そして、証明書データL65はソフトウェア利用者に提供され、証明書データL65の中のメッセージM63とデジタル署名S64とは、公開されている公開鍵E62と暗号化アルゴリズムCとを利用してメッセージM'66（ $M' = C(E, S)$ ）を計算する（ステップS74）。メッセージM63とメッセージM'

66とを比較し（ステップS75）、両者が一致するかどうか判定する（ステップS76）。両者が一致する場合は、デジタル署名S64は正当なものと認められ（ステップS77）、両者が一致しなければ、デジタル署名S64は不当なものとして、メッセージM63は破棄される（ステップS78）。

【0025】

証明書データL65に改ざん、偽造がなければ、秘密鍵D61と一対である公開鍵E62によってデジタル署名S64の正当性が確認されると同時に、このデジタル署名S64は秘密鍵D61によって、メッセージM63から作られたものであることが確認される。従って、ソフトウェア利用者はメッセージM63をソフトウェア作成者からの正しいデータとして受け入れることが可能となる。

【0026】

この公開鍵暗号方式の認証の原理に基づいて、本実施形態のソフトウェア管理システムは構成される。

【0027】

以下、本実施形態におけるソフトウェア管理システム1について、図1～図8を用いて説明する。

【0028】

まず、本実施形態におけるソフトウェア管理システム1の構成について、図1を用いて説明する。

【0029】

本実施形態におけるソフトウェア管理システム1は、製品管理サーバ2、ルートサーバ3、認証サーバ4、およびユーザ端末5から構成され、それぞれ構内LAN、専用線、インターネット7等のネットワーク6によって相互に接続される。図1では、各サーバ2～4はLAN等のネットワーク6によって接続されているが、それぞれインターネット7を介して接続されてもよい。また、製品管理サーバ2は、製品（ソフトウェア）を梱包して出荷する工場に設置され、ルートサーバ3は、セキュリティの確保しやすい場所に設置することが望ましい。

【0030】

また、製品管理サーバ2は製品管理情報データベース8を、ルートサーバ3は

ルート情報データベース 9 を、認証サーバ 4 は認証情報データベース 1 0 をそれぞれ備える。

【 0 0 3 1 】

製品管理サーバ 2 が備える製品管理情報データベース 8 には、ライセンス秘密鍵 2 1、ライセンス公開鍵 2 2、製品番号 2 3、製品のシリアルナンバー 2 4、ライセンスコード 2 5 が記録される。また、ルートサーバ 3 が備えるルート情報データベース 9 には、ルート秘密鍵 3 1、ルート公開鍵 3 2 が記録される。

【 0 0 3 2 】

また、認証サーバ 4 が備える認証情報データベース 1 0 には、アクティベーション秘密鍵 4 1、アクティベーション公開鍵 4 2、ライセンスキー証明書データ 4 3、サーバ有効期限 4 4、認証サーバ証明書データ 4 5、アクティベーション情報 4 6、ソフト有効期限 4 7 が記録される。

【 0 0 3 3 】

ライセンス秘密鍵 2 1、ライセンス公開鍵 2 2、ルート秘密鍵 3 1、ルート公開鍵 3 2、アクティベーション秘密鍵 4 1、アクティベーション公開鍵 4 2 は、例えば、R S A 方式で設計される。

【 0 0 3 4 】

また、認証情報データベース 1 0 に記録されるアクティベーション情報 4 6 は、図 2 に示すように、ユーザ端末 5 から送信される製品番号 2 3、シリアルナンバー 2 4、ライセンスコード 2 5、M A C アドレス (Media Access Control Address) を記録するデータテーブルである。

【 0 0 3 5 】

なお、製品管理サーバ 2、ルートサーバ 3、認証サーバ 4、およびユーザ端末 5 は、いずれもそれぞれの処理にあわせた暗号化プログラム、および復号化プログラムを予め有することとする。すなわち、製品管理サーバ 2 は、ライセンス秘密鍵に対応した復号化プログラムを有し、ルートサーバ 3 は、ルート公開鍵に対応した復号化プログラムを有し、認証サーバ 4 は、ルート公開鍵に対応した暗号化プログラムと、ライセンス公開鍵に対応した暗号化プログラムと、アクティベーション公開鍵に対応した復号化プログラムとを有し、ユーザ端末 5 は、ルート

公開鍵に対応した暗号化プログラムと、アクティベーション公開鍵に対応して暗号化プログラムを有し、デジタル書名を作成する際、およびデジタル署名を複合する際に用いられる。

【0036】

<製品管理サーバの処理手順>

次に、製品管理サーバ2の処理手順について、図3を用いて説明する。

【0037】

工場からソフトウェアを出荷する際には、製品管理サーバ2では、個々の製品を区別して生産の管理や販売の管理、サポートの管理を行えるよう、製品にシリアルナンバー24を発行し、個々の製品に付加している。シリアルナンバー24は年月日、連番などを組み合わせて作成され、製品管理情報データベース8に記録される。例えば、YY/MM/連番で構成され、2002年12月のひとつめの出荷分に対して、「2002120001」といった番号が作られる。

【0038】

また、製品の種類を区別して生産の管理や販売の管理、サポートの管理を行えるよう製品番号23が作成され、製品管理情報データベース8に記録される。このソフトウェアの製品番号23は、例えば「SW-1000」とする。

【0039】

まず、製品管理サーバ2は、ライセンス公開鍵22を製品管理情報データベース8から取得して、ルートサーバ3に送信しておく（ステップS01）。

【0040】

次に、製品管理サーバ2は、製品番号23、シリアルナンバー24、およびライセンス秘密鍵21を製品管理情報データベース8から取得して、この製品番号23、シリアルナンバー24、およびライセンス秘密鍵21を用いてデジタル署名を作成する（ステップS02）。そして、製品管理サーバ2は、このデジタル署名をライセンスコード25として製品管理情報データベース8に記録する。

【0041】

また、この製品管理サーバ2にはプリンタ等の印刷装置（図示しない）が接続されており、製品管理サーバ2は、製品に添付する保証書に製品番号23、シリ

アルナンバー 2 4、およびライセンスコード 2 5 を印刷するよう印刷装置に指示を出す（ステップ S 0 3）。そしてこれらを印刷した保証書をソフトウェアに添付して梱包し、出荷する。

【 0 0 4 2 】

＜ルートサーバの処理手順＞

次に、ルートサーバ 3 の処理手順について、図 4 を用いて説明する。

【 0 0 4 3 】

まず、ルートサーバ 3 は、ルート情報データベース 9 からルート公開鍵 3 2 を取得し、認証サーバ 4 に送信する（ステップ S 1 1）。

【 0 0 4 4 】

次に、ルートサーバ 3 は、製品管理サーバ 2 からライセンス公開鍵 2 2 を受信すると（ステップ S 1 2）、ルート情報データベース 9 からルート秘密鍵 3 1 を取得し、そのライセンス公開鍵 2 2 とルート秘密鍵 3 1 とを用いてデジタル署名を作成し（ステップ S 1 3）、ライセンス公開鍵 2 2 とデジタル署名とをまとめた証明書データを作成する。ルートサーバ 3 は、この証明書データをライセンスキー証明書データ 4 3 として認証サーバ 4 に送信する（ステップ S 1 4）。

【 0 0 4 5 】

また、ルートサーバ 3 は、認証サーバ 4 からサーバ有効期限 4 4 とアクティベーション公開鍵 4 2 を受信すると（ステップ S 1 5）、ルートサーバ 3 は、サーバ有効期限 4 4 とアクティベーション公開鍵 4 2 とルート秘密鍵 3 1 とを用いてデジタル署名を作成し（ステップ S 1 6）、サーバ有効期限 4 4 とアクティベーション公開鍵 4 2 とデジタル署名とをまとめた証明書データを作成する。ルートサーバ 3 は、この証明書データを認証サーバ証明書データ 4 5 として認証サーバ 4 に送信する（ステップ S 1 7）。

【 0 0 4 6 】

なお、認証作業の簡略化のため、サーバ有効期限 4 4 は用いなくてもよい。

【 0 0 4 7 】

＜認証サーバの処理手順＞

次に、認証サーバ 4 の処理手順について、図 5 を用いて説明する。

【 0 0 4 8 】

まず、認証サーバ 4 は、ルートサーバ 3 からルート公開鍵 3 2 を受信する（ステップ S 2 1）。また、認証サーバ 4 は、ルートサーバ 3 からライセンスキー証明書データ 4 3 を受信する（ステップ S 2 2）。

【 0 0 4 9 】

次に、認証サーバ 4 は、このルート公開鍵 3 2 を用いてライセンスキー証明書データ 4 3 中のデジタル署名の正当性を判定し、ライセンス公開鍵 2 2 が受け入れ可能であるか判定する（ステップ S 2 3）。ルート公開鍵 3 2 とライセンスキー証明書データ 4 3 中のデジタル署名とから作成されるライセンス公開鍵 2 2 と、ライセンスキー証明書データ 4 3 中のライセンス公開鍵 2 2 とが一致すると判定されると、デジタル署名の正当性が承認されたことになり、以後は、認証サーバ 4 は、このライセンス公開鍵 2 2 を使用する。デジタル署名とライセンス公開鍵 2 2 のどちらか一方でも改ざん、偽造などされている場合は、承認されず拒絶されるので、認証サーバ 4 は警告を表示して作業を終了する。

【 0 0 5 0 】

また、認証サーバ 4 は、認証情報データベース 1 0 からデジタル署名のサーバ有効期限 4 4 を設定し、認証情報データベース 1 0 に記録する。このサーバ有効期限 4 4 は、例えば、現在の日付の属する月の 3 ヶ月後の月末とする。即ち、2 0 0 3 年 1 月 1 日時点でのサーバ有効期限 4 4 は 2 0 0 3 年 4 月 3 0 日である。サーバ有効期限 4 4 は毎月 1 日に更新される。

【 0 0 5 1 】

認証サーバ 4 は、設定されたサーバ有効期限 4 4 とアクティベーション公開鍵 4 2 とを認証情報データベース 1 0 から取得し、ルートサーバ 3 へ送信する（ステップ S 2 4）。

【 0 0 5 2 】

また、ルートサーバ 3 から認証サーバ証明書データ 4 5 が送信されると、認証サーバ 4 は、その認証サーバ証明書データ 4 5 を受信し、認証情報データベース 1 0 に記録する（ステップ S 2 5）。

【 0 0 5 3 】

なお、認証作業の簡略化のため、サーバ有効期限 44 を設定しなくてもよい。

【0054】

以上、製品管理サーバ2、ルートサーバ3、および認証サーバ4の各処理手順をまとめると、図6のシーケンス図のようになる。図6に示す一連の処理が、ソフトウェアの出荷段階で行われる。

【0055】

＜ユーザ端末5のアクティベーション処理手順＞

次に、ユーザ端末5から行われるアクティベーション処理について、図7～図8に基づいて説明する。

【0056】

まず、ユーザは自分のユーザ端末5に購入したソフトウェアをインストールする。ソフトウェアを正規のものと確認し機能制限を解除し、警告表示を停止することをアクティベーションと呼ぶ。この段階ではアクティベーションがされていないのでソフトウェアは完全には機能しない。

【0057】

しかし、ソフトウェアはPCの環境によって動作しなかったり処理速度に問題が生じたりすることがあるので、アクティベーションする前でも一部の機能制限をした状態で使用可能としたり、アクティベーションを行うよう警告を表示しながら使用可能としたりして、予め動作確認が可能としておくのが望ましい。

【0058】

ユーザは、ソフトウェアの動作に問題がないことを確認した上で、アクティベーションを開始する。ユーザ端末5でソフトウェアが起動されると、図8(a)に示すようなアクティベーションするかどうかを確認する画面が表示される。この図8(a)の画面で「はい」のボタンをクリックすると(ステップS31)、ユーザ端末5は、まず自身のMACアドレスを取得する(ステップS32)。

【0059】

MACアドレスとは、ネットワーク6でホストを識別するために設定されるハードウェアアドレスであり、Ethernet(登録商標)では、ネットワーク6に接続するデバイスであるNIC(Network Interface Card)に対して48ビットの識別

符号が付けられており、Ethernet（登録商標）アドレスとも呼ぶ。48ビットのうち前半24ビットがIEEE（Institute of Electrical and Electronic Engineers）で管理されたベンダー固有のIDで、後半24ビットが各NICの連番となり、世界中に1つしかないユニークな番号になる。このMACアドレスによってユーザ端末5を特定することができる。

【0060】

ここで取得されるMACアドレスは、例えば、12桁の16進数「00-80-88-41-01-A0」といった形で表される。

【0061】

そして、図8（b）の入力画面で、ユーザがソフトウェアに添付された保証書に記載されているシリアルナンバー24、製品番号23、ライセンスコード25を入力し、「送信」のボタンをクリックすると（ステップS33）、ユーザ端末5は、先に取得したMACアドレスと、シリアルナンバー24、製品番号23、ライセンスコード25を、インターネット7を介して認証サーバ4に送信する（ステップS34）。なお、ユーザが自らMACアドレスを入力するようにしてもよい。

【0062】

一方、認証サーバ4は、ユーザ端末5からシリアルナンバー24、製品番号23、ライセンスコード25、およびMACアドレスを受信すると、まず、ライセンス公開鍵22を用いてライセンスコード25の正当性について判定し、製品番号23、シリアルナンバー24が受け入れ可能であるか判定する（ステップS35）。ライセンス公開鍵22は、予めルート公開鍵32によって正当なものと判定されているので、これを用いて判定を行うことができる。

【0063】

認証サーバ4は、ライセンス公開鍵22とライセンスコード25（デジタル署名）を用いて、シリアルナンバー24と製品番号23を復号する。認証サーバ4は、ライセンスコード25から復号されるシリアルナンバー24、および製品番号23と、ユーザ端末5から送信されるシリアルナンバー24、および製品番号23とを比較し、両者が一致すると判定すると、ライセンスコード25の正当性

が承認されたことになり、製品番号 23、シリアルナンバー 24 を受け入れる。

【0064】

また、逆に認証サーバ 4 が、ライセンスコード 25 を正当なものと判定しなければデータに改ざん、偽造などがあったものとして警告を表示し、作業を終了する。

【0065】

次に、製品番号 23、シリアルナンバー 24、ライセンスコード 25 の正当性が承認されると、アクティベーション情報 46 との照合が行われる。アクティベーション情報 46 には、ライセンスコード 25、製品番号 23、シリアルナンバー 24、MAC アドレスを記録するレコードが、アクティベーションの度に生成され、記憶される。

【0066】

そこでまず、認証サーバ 4 は、正当性が承認されたライセンスコード 25 と同じライセンスコード 25 を記録しているレコードを、下記の条件をもって抽出する（ステップ S36）。

【0067】

条件 1：同一のライセンスコード 25 が記録されているレコードが存在しない。

【0068】

条件 2：ライセンスコード 25 が一致し、かつ MAC アドレスが一致するレコードが存在する。

【0069】

条件 3：ライセンスコード 25 は一致するが、MAC アドレスの異なるレコードの数が 2 以下である。

【0070】

以上、3つの条件のうち、ひとつでも該当すれば（ステップ S37）、認証サーバ 4 は、ユーザ端末 5 から送られた製品番号 23、シリアルナンバー 24、ライセンスコード 25、および MAC アドレスを新たなレコードとしてアクティベーション情報 46 に記録する（ステップ S38）。なお、ライセンスコード 25 が一致し、かつ MAC アドレスが一致する場合のみ、アクティベーション情報 4

6 への記録は行わない。また、3 つの条件をすべて満たさない場合は、認証サーバ 4 は、アクティベーション情報 4 6 への記録を行わず、作業を終了する（ステップ S 3 9）。

【 0 0 7 1 】

なお、何等かの事情で 4 回目のアクティベーションを必要とするユーザは、電話などの手段でサービスセンターに連絡し、事情が確認されればアクティベーション情報 4 6 の該当レコードを削除してもらってから、再度アクティベーションを行う。

【 0 0 7 2 】

また、認証サーバ 4 は、ソフトウェアの使用期限を示すソフト有効期限 4 7 を設定する（ステップ S 4 0）。ソフト有効期限 4 7 は例えば現在の日付の属する月の 6 ヶ月後の月末とする。即ち、2 0 0 3 年 1 月 1 日時点でのソフト有効期限 4 7 は 2 0 0 3 年 7 月 3 1 日である。ソフト有効期限 4 7 は毎月 1 日に更新される。

【 0 0 7 3 】

次に、認証サーバ 4 は、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、ライセンスコード 2 5 とアクティベーション秘密鍵 4 1 を用いてデジタル署名を作成し（ステップ S 4 1）、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、ライセンスコード 2 5、認証サーバ証明書データ 4 5 と、作成したデジタル署名とをあわせた証明書データを作成する。認証サーバ 4 は、この証明書データをアクティベーションコードとして認証情報データベース 1 0 に記録し、ユーザ端末 5 に送信する（ステップ S 4 2）。

【 0 0 7 4 】

なお、認証作業の簡略化のためソフト有効期限 4 7 を設定しない場合は、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ライセンスコード 2 5 とアクティベーション秘密鍵 4 1 を用いてデジタル署名を作成し、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、認証サーバ証明書データ 4 5 と、作成したデジタル署名とをあわせたアクティベーションコードを作成する。

【0075】

ユーザ端末5は、認証サーバ4からアクティベーションコードを受信すると、インターネット7を介してルートサーバ3にアクセスして、ルート公開鍵32を取得する（ステップS43）。

【0076】

まず、ユーザ端末5は、アクティベーションコードから認証サーバ証明書データ45を抽出し、ルート公開鍵32を用いて認証サーバ証明書データ45中のデジタル署名の正当性を判定し、アクティベーション公開鍵42、サーバ有効期限44が受け入れ可能であるか判定する（ステップS44）。判定処理の簡略化のためサーバ有効期限44を設定しない場合は、ルート公開鍵32を用いて認証サーバ証明書データ45中のデジタル署名の正当性を判定し、アクティベーション公開鍵42が受け入れ可能であるか判定する。

【0077】

ユーザ端末5は、ルート公開鍵32と認証サーバ証明書データ45中のデジタル署名を用いて、アクティベーション公開鍵42とサーバ有効期限44を復号する。ユーザ端末5は、認証サーバ証明書データ45中のデジタル署名から復号されるアクティベーション公開鍵42、およびサーバ有効期限44と、認証サーバ証明書データ45中のアクティベーション公開鍵42、およびサーバ有効期限44とを比較し、両者が一致すると判定すると、認証サーバ証明書データ45中のデジタル署名の正当性が承認されたことになり、アクティベーション公開鍵42とサーバ有効期限44を受け入れる。

【0078】

また、逆に認証サーバ4が、認証サーバ証明書データ45中のデジタル署名を正当なものと判定しなければデータに改ざん、偽造などがあったものとして警告を表示し、作業を終了する。

【0079】

次に、ユーザ端末5は、サーバ有効期限44と現在の日付とを比較し（ステップS45）、現在の日付が有効期限内であれば次のステップに進み、有効期限外であれば警告を表示して作業を終了する（ステップS46）。仮に認証サーバ証

明書データ 4 5 が盗難されても、その認証サーバ証明書データ 4 5 は、サーバ有効期限 4 4 が切れると使用できなくなるので、不正使用を最小限にとどめることができる。なお、判定処理の簡略化のためサーバ有効期限 4 4 が設定されていない場合は、ユーザ端末 5 はこの処理を行わない。

【0 0 8 0】

次に、ユーザ端末 5 は、先に正当なデータであると承認されたアクティベーション公開鍵 4 2 を用いてライセンスコード 2 5 の正当性を判定し、アクティベーションコード中の製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7 が受け入れ可能であるか判定する（ステップ S 4 7）。

【0 0 8 1】

ユーザ端末 5 は、アクティベーション公開鍵 4 2 とアクティベーションコード中のデジタル署名を用いて、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、ライセンスコード 2 5 を復号する。ユーザ端末 5 は、アクティベーションコード中のデジタル署名から復号される製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、およびライセンスコード 2 5 と、アクティベーションコード中の製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、およびライセンスコード 2 5 とを比較し、両者が一致すると判定すると、アクティベーションコード中のデジタル署名の正当性が承認されたことになり、製品番号 2 3、シリアルナンバー 2 4、MAC アドレス、ソフト有効期限 4 7、ライセンスコード 2 5 を受け入れる。

【0 0 8 2】

また逆に認証サーバ 4 が、アクティベーションコード中のデジタル署名を正当なものと判定しなければデータに改ざん、偽造などがあったものとして警告を表示し、作業を終了する。

【0 0 8 3】

ユーザ端末 5 は、アクティベーションコード中の製品番号 2 3、シリアルナンバー 2 4、ライセンスコード 2 5、MAC アドレスと、先に入力し認証サーバ 4 に送信した製品番号 2 3、シリアルナンバー 2 4、ライセンスコード 2 5、MAC アドレスとを比較し、データの誤配信や違う端末向けの認証の盗用等を検出す

る（ステップS48）。

【0084】

全ての判定処理が終了すると、ユーザ端末5は、ソフト有効期限47をそのソフトウェアの使用期限として、ソフトウェアの全ての機能が実行可能になるよう機能制限を解除し、警告表示を停止する（ステップS49）。また、ソフト有効期限47が設定されていない場合は、無期限でソフトウェアの全ての機能が実行可能になるよう機能制限を解除し、警告表示を停止する。

【0085】

これによって一連のアクティベーション作業がすべて完了する。

【0086】

このように、ソフトウェアの製品番号23、シリアルナンバー24、製品管理サーバ2で用いられる暗号鍵、認証サーバ4で用いられる暗号鍵がルートサーバ3によって認証されるので、単にソフトウェアの製品番号23、シリアルナンバー24の改ざンだけでなく、製品管理サーバ2で用いられる暗号鍵、認証サーバ4で用いられる暗号鍵、アクティベーションコードの偽造、改ざンにも対処できる強固な認証システムが形成される。

【0087】

なお、上記実施形態では、RSA方式の暗号鍵の例を説明したが、公開鍵暗号方式にはRSAの他にもDSA（Digital Signature Algorithm）、ElGamalなどがあり、RSA以外の公開鍵暗号方式であってもよい。

【0088】

また、認証サーバ証明書データ45を、その正当性を判定する度にユーザ端末5に送信し、ユーザ端末5にてルートサーバ3の公開鍵で正当性を判定しているので、認証サーバ4を変更したり、認証サーバ4のアクティベーション公開鍵42・アクティベーション秘密鍵41を変更したりしても、そのままシステムを使用することができる。さらに、サーバ有効期限44を設定しているので、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたサーバ有効期限44で無効となるので、不正使用を一時的なものにすることができる。

【0089】

ただし、正当性の判定作業の煩雑さと不正防止効果とを比較衡量した上で、正当性の判定作業の負担軽減を優先する場合は、認証サーバ 4 でサーバ有効期限 4 4 を設定せず、ユーザ端末 5 においてもサーバ有効期限 4 4 と現在の日付との照合を行わないようにしても良い。

【 0 0 9 0 】

また、ソフト有効期限 4 7 が切れると再びアクティベーションを促すようにしておけば、ユーザは再びアクティベーションを行うこととなり、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたソフト有効期限 4 7 で機能が停止するので、不正使用を一時的なものにすることができる。

【 0 0 9 1 】

ただし、ユーザの操作の煩雑さと不正使用の防止効果とを比較衡量した上で、ユーザの負担軽減を優先する場合は、認証サーバ 4 でソフト有効期限 4 7 を設定せず、ユーザ端末 5 では無期限のアクティベーションと許可するようにしても良い。

【 0 0 9 2 】

また、上記実施形態では、ライセンスキー証明書データ 4 3（製品管理サーバ 2 のデジタル署名と製品管理サーバ 2 のライセンス公開鍵 2 2）をデジタル署名後に認証サーバ 4 に送る例を示したが、ライセンスキー証明書データ 4 3 を製品管理サーバ 2 に送り返してソフトウェア製品に添付して出荷しても良い。この場合、アクティベーション時に、ユーザ端末 5 から認証サーバ 4 にライセンスキー証明書データ 4 3 を送ることとなる。

【 0 0 9 3 】

この場合、製品管理サーバ 2 を複数所有したり、増設したり、製品管理サーバ 2 が用いる暗号鍵を更新したりしても、暗号鍵の種類を意識せず、そのままシステムを使用することができる長所がある。

【 0 0 9 4 】

また、上記実施形態では、ユーザ端末 5 がルートサーバ 3 のルート公開鍵 3 2 を入手する方法として、ユーザ端末 5 が認証作業の時にルートサーバ 3 に要求し、ルートサーバ 3 から送られる例を示したが、これに限定されるものではなく、

例えば、予めソフトウェアの内部にルートサーバ3のルート公開鍵32が記憶されていてもよい。

【0095】

また、上記実施形態では、ユーザ端末5固有の番号としてMACアドレスを使用する例を示したが、これに限定されるものではなく、例えば、MACアドレスにチェックサムなどを付加したものや、プロセッサのシリアルナンバー、ハードディスクのID、それらを組み合わせたもの等、ユーザ端末5を特定できる番号であればよい。

【0096】

【発明の効果】

以上詳細に説明したように、本発明によれば、ソフトウェア固有の識別コードやユーザ端末固有の端末コードを用いて、製品管理サーバの暗号鍵と認証サーバの暗号鍵をルートサーバで認証してから使用するので、ソフトウェアの偽造、改ざんだけでなく、暗号鍵の偽造、改ざん、偽の製品管理サーバ、偽の認証サーバなどに対しても対抗できる、不正行為を防止するソフトウェアのライセンス管理が可能となる。

【0097】

また、第3のデジタル署名の有効期限を示すサーバ有効期限を設定しているので、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたサーバ有効期限で無効となるので、不正使用を一時的なものにすることができる。

【0098】

さらに、ソフトウェアの使用期限を示すソフト有効期限が切れると再びアクティベーションを促すようにしておけば、ユーザは再びアクティベーションを行うこととなり、たとえ予想外の偽造、改ざんに類する行為があったとしても、設定されたソフト有効期限で機能が停止するので、不正使用を一時的なものにすることができる。

【図面の簡単な説明】

【図1】

本発明のソフトウェア管理システムの構成を示す図である。

【図 2】

アクティベーション情報を示すデータテーブルである。

【図 3】

製品管理サーバの処理手順を示すフローチャートである。

【図 4】

ルートサーバの処理手順を示すフローチャートである。

【図 5】

認証サーバの処理手順を示すフローチャートである。

【図 6】

製品管理サーバ、ルートサーバ、認証サーバの処理手順の関係を示すシーケンス図である。

【図 7】

ユーザ端末と認証サーバの処理手順を示すシーメンス図である。

【図 8】

ユーザ端末でアクティベーションを行なう際に表示される画面例である。

【図 9】

公開鍵暗号方式によるデジタル署名と認証の処理手順を示すフローチャートである。

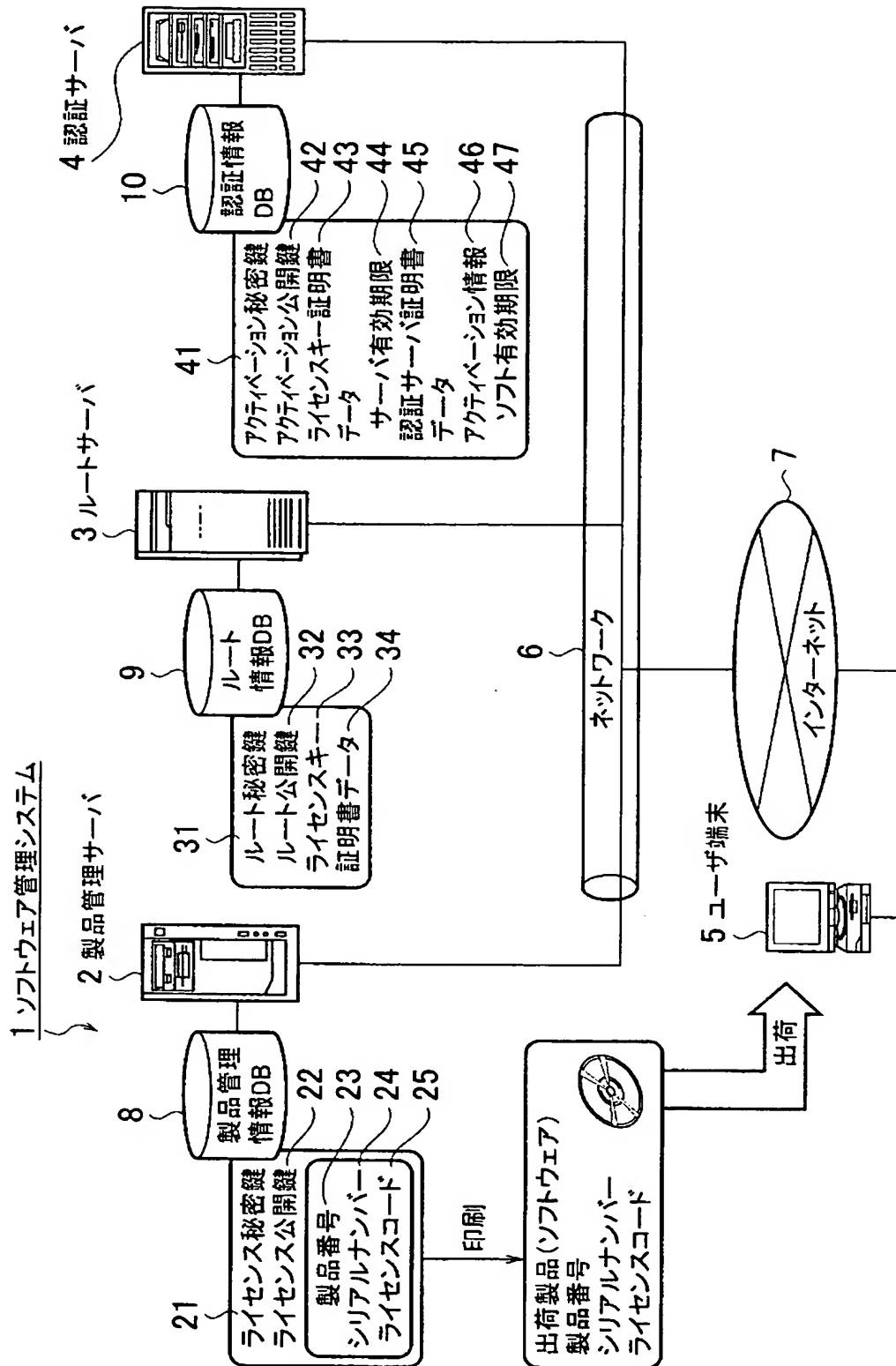
【符号の説明】

- 1 ソフトウェア管理システム
- 2 製品管理サーバ
- 3 ルートサーバ
- 4 認証サーバ
- 5 ユーザ端末
- 6 ネットワーク
- 7 インターネット
- 8 製品管理情報データベース
- 9 ルート情報データベース
- 10 認証情報データベース

- 2 1 ライセンス秘密鍵
- 2 2 ライセンス公開鍵
- 2 3 製品番号
- 2 4 シリアルナンバー
- 2 5 ライセンスコード
- 3 1 ルート秘密鍵
- 3 2 ルート公開鍵
- 4 1 アクティベーション秘密鍵
- 4 2 アクティベーション公開鍵
- 4 3 ライセンスキー証明書データ
- 4 4 サーバ有効期限
- 4 5 認証サーバ証明書データ
- 4 6 アクティベーション情報
- 4 7 ソフト有効期限
- 6 1 秘密鍵 D
- 6 2 公開鍵 E
- 6 3 メッセージ M
- 6 4 デジタル署名 S
- 6 5 証明書データ L
- 6 6 メッセージ M'

【書類名】 図面

【図 1】

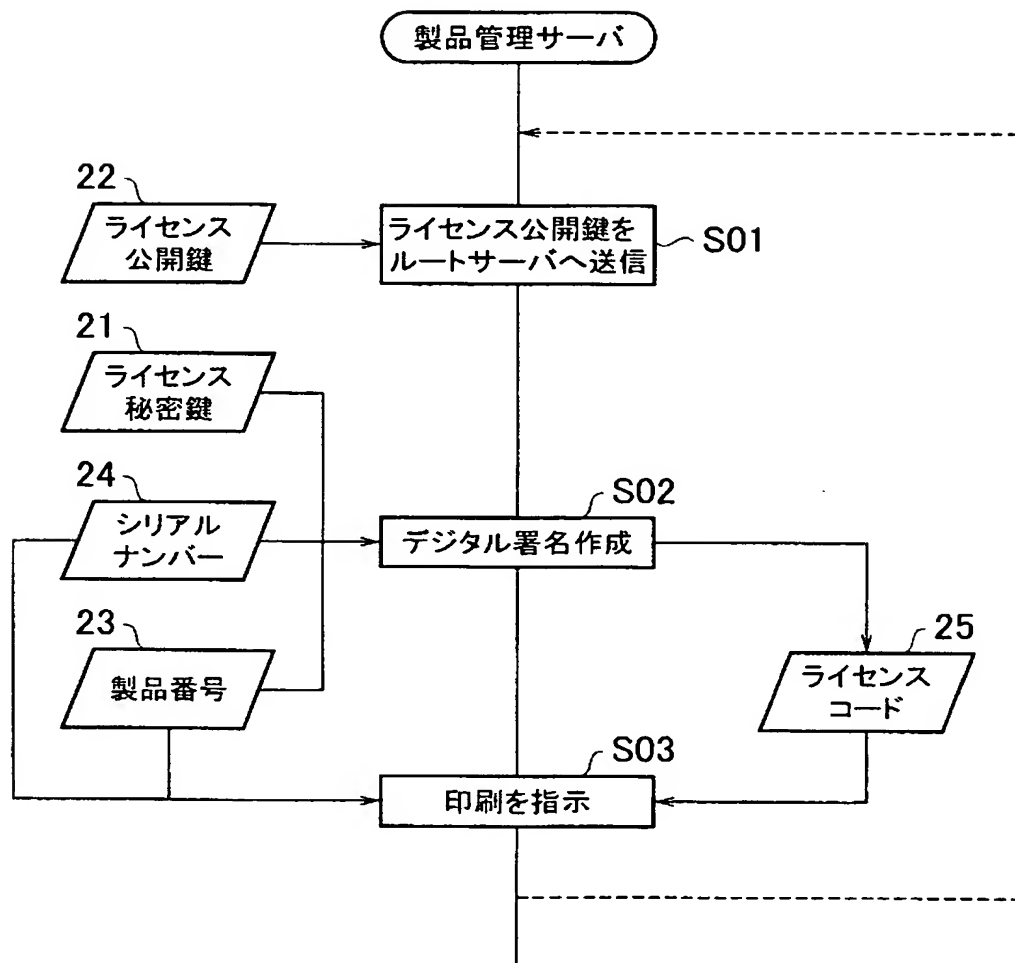


【図 2】

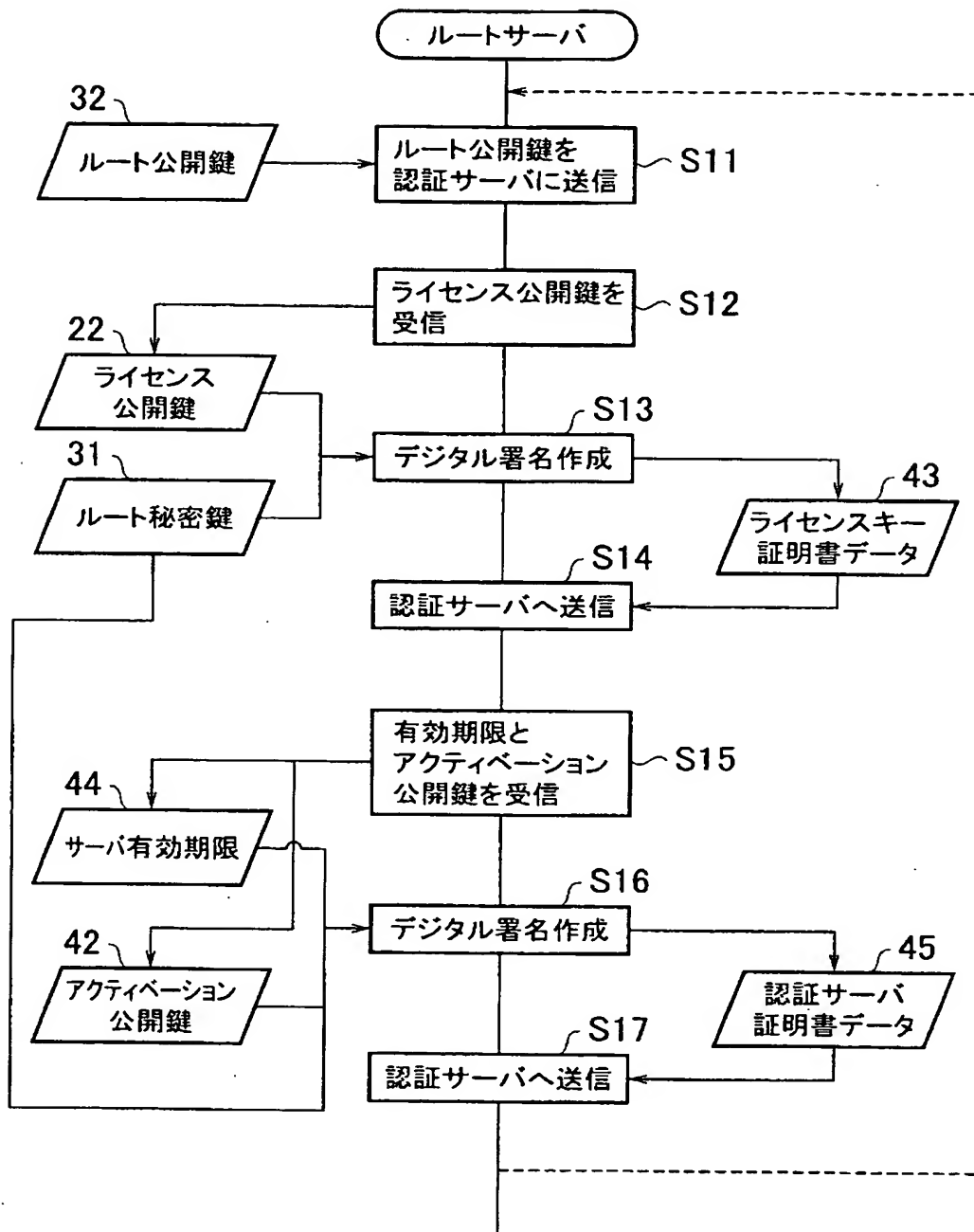
アクティベーション情報

ライセンスコード	製品番号	シリアルナンバー	MACアドレス
a0857f05e8f0	SW-1000	2002120001	00-80-88-41-01-a0
7ra3vds78a9g8	SW-1000	2002120013	00-80-88-b1-51-91
32ehau583681	SW-1000	2002120657	00-80-88-41-11-a2
48y3581dsth84	SW-1000	2002120987	00-80-88-46-a1-18
:	:	:	:

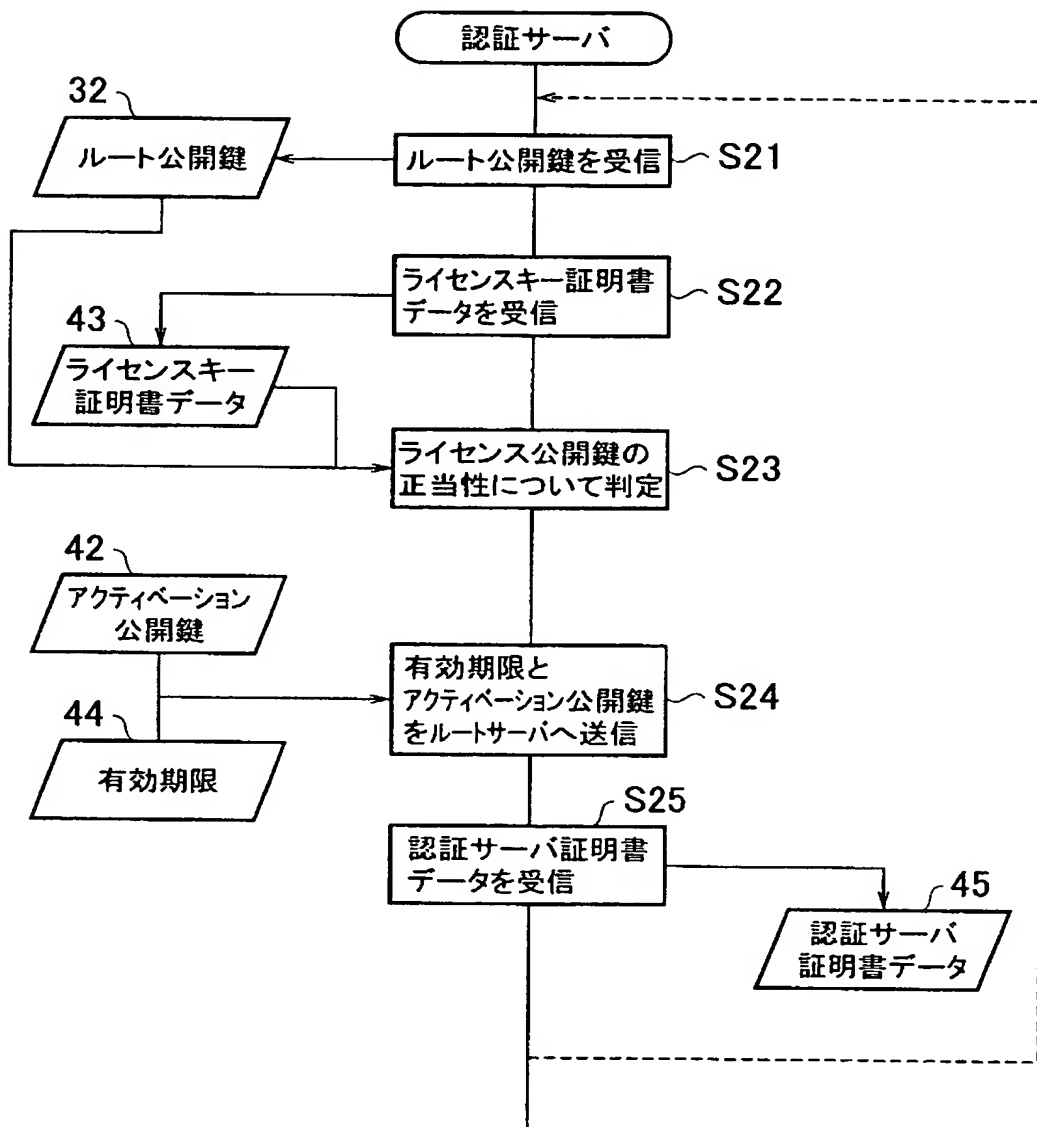
【図 3】



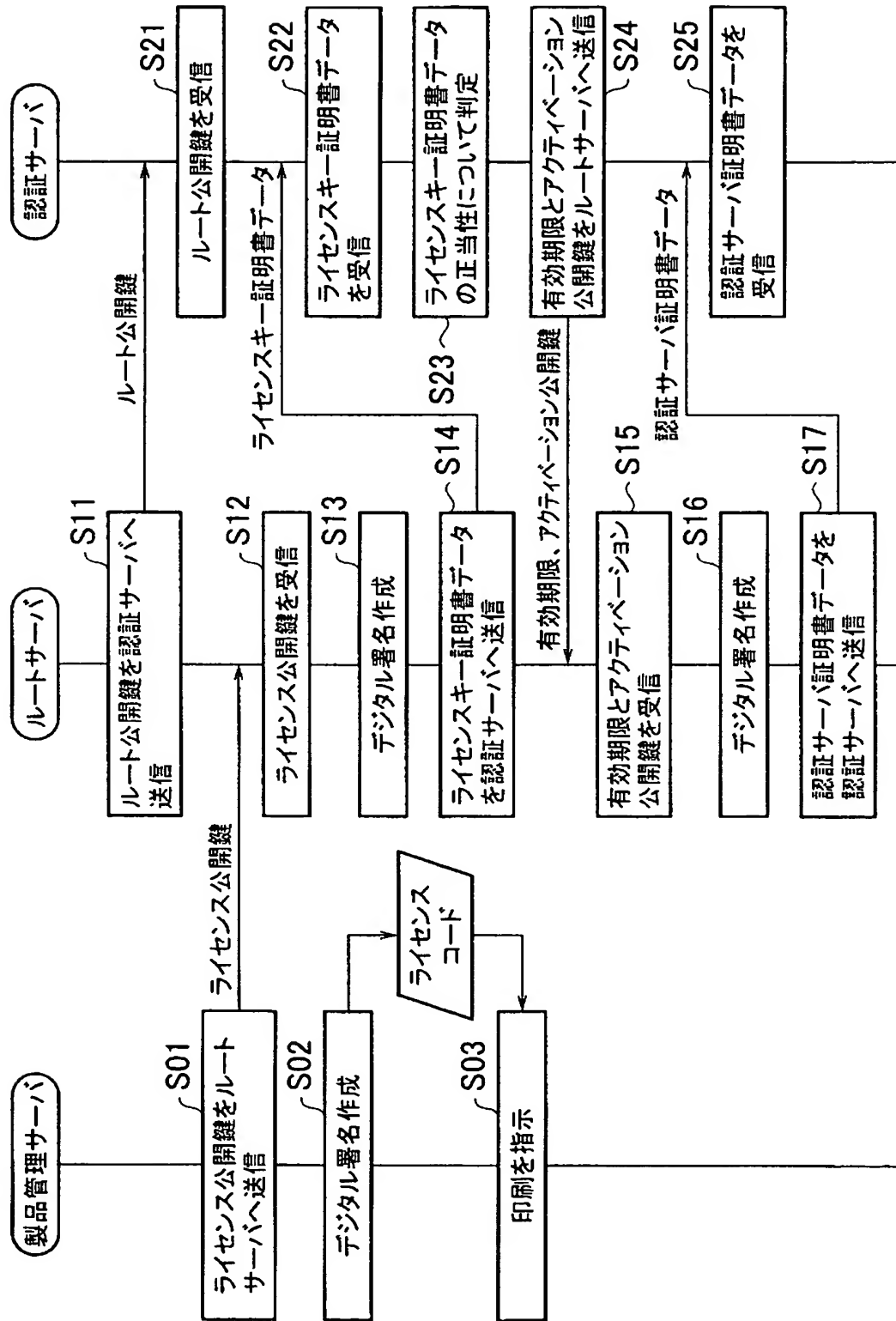
【図 4】



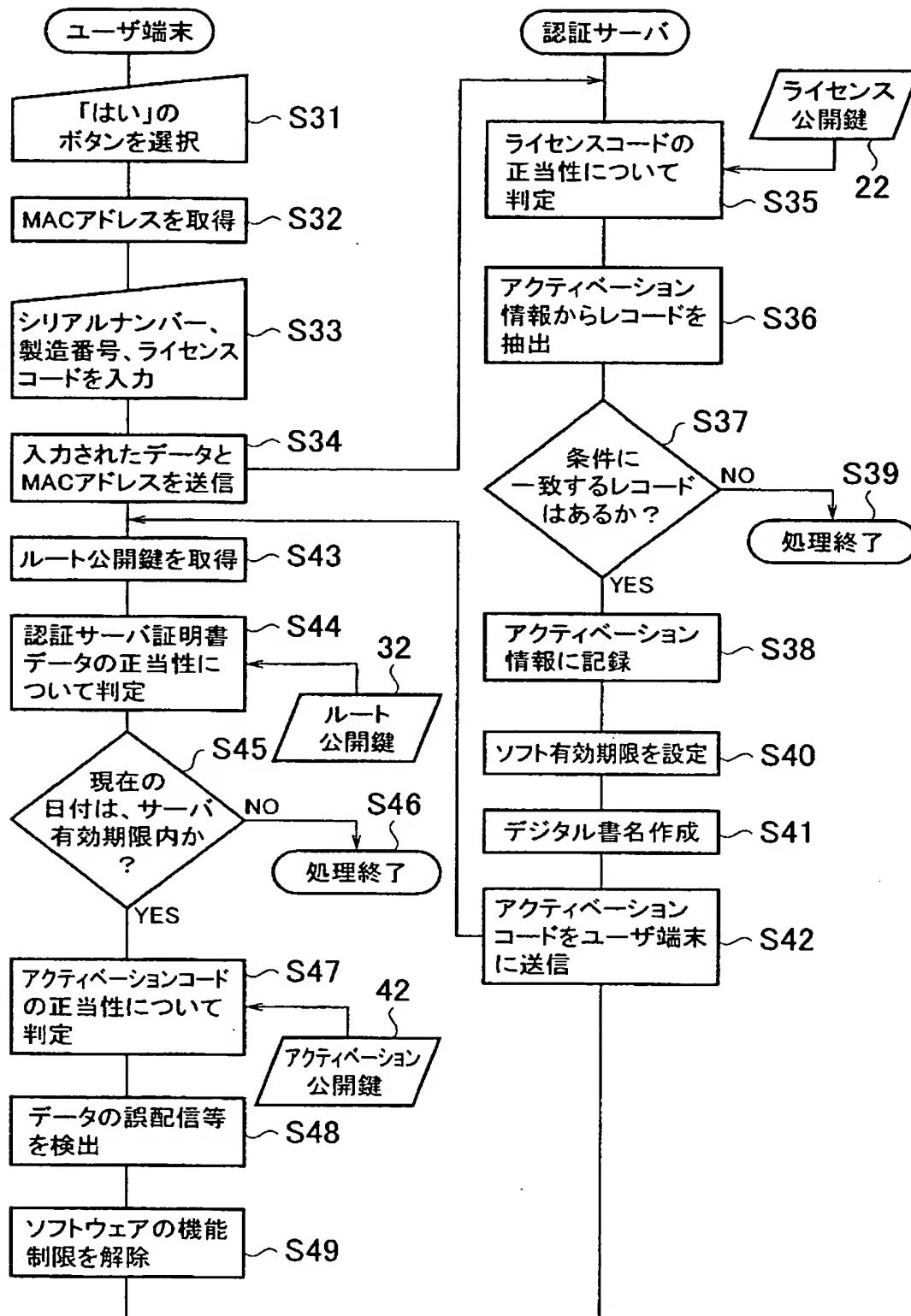
【図 5】



【図 6】

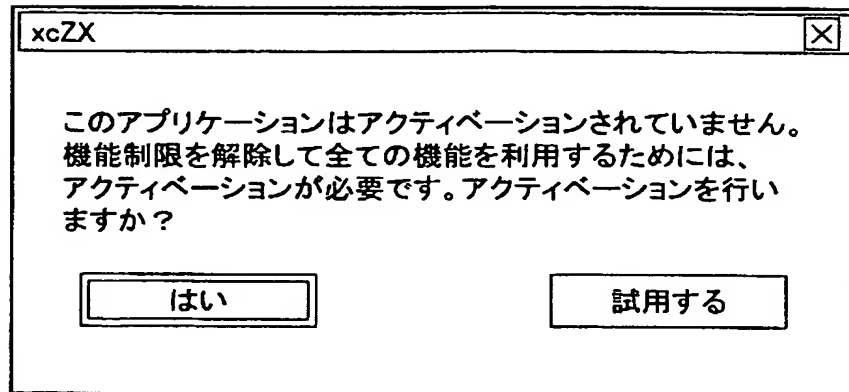


【図 7】



【図 8】

(a)

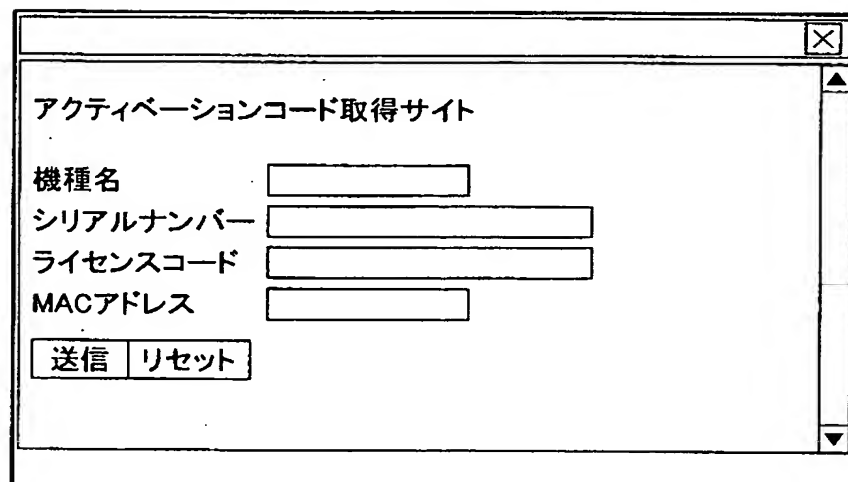


xcZX

このアプリケーションはアクティベーションされていません。
機能制限を解除して全ての機能を利用するためには、
アクティベーションが必要です。アクティベーションを行いますか？

はい 試用する

(b)



アクティベーションコード取得サイト

機種名

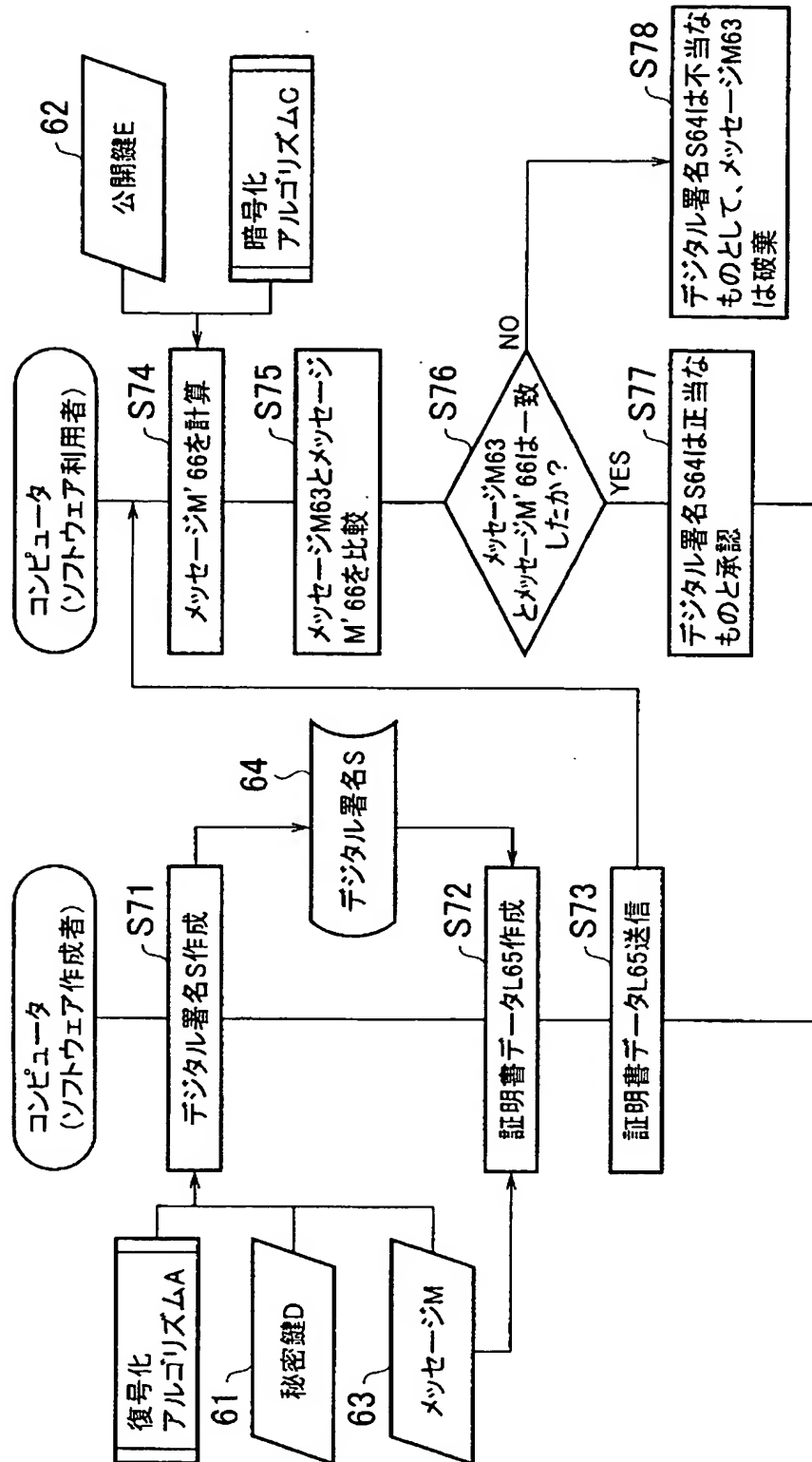
シリアルナンバー

ライセンスコード

MACアドレス

送信 リセット

【図 9】



【書類名】 要約書

【要約】

【課題】 ソフトウェアのライセンス管理を公開鍵暗号方式の暗号鍵を用いて行うライセンス管理方法、およびライセンス管理システムを提供する。

【解決手段】 製品管理サーバ2は、ライセンス秘密鍵21と識別コードから製品に付される第1のデジタル署名を作成し、ルートサーバ3は、ルート秘密鍵31とライセンス公開鍵22から第2のデジタル署名を、アクティベーション公開鍵42から第3のデジタル署名を作成し、認証サーバ4は、第2のデジタル署名と、ライセンス公開鍵21の正当性と、第1のデジタル署名と識別コードの正当性を判定し、アクティベーション秘密鍵41と製品コードと端末コードとから第4のデジタル署名を作成し、ユーザ端末5は、第4のデジタル署名とアクティベーション公開鍵42の正当性と、第4のデジタル署名と製品識別コードと端末コードとの正当性を判定し、判定結果に基づいて、ソフトウェアの機能制限を解除する。

【選択図】 図1

特願 2 0 0 2 - 3 7 4 9 7 0

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 3 2 9]

1. 変更年月日

1 9 9 0 年 8 月 8 日

[変更理由]

新規登録

住 所

神奈川県横浜市神奈川区守屋町 3 丁目 1 2 番地

氏 名

日本ビクター株式会社